Articles and Reports

These are articles and reports available online that are closely related to BSI topics.

Name	Publication Date	Abstract
A Software Flaw Taxonomy: Aiming Tools at Security	2/19/08	Sam Weber, Paul A. Karger, and Amit Paradkar. *Proceedings of Software Engineering for Secure Systems – Building Trustworthy Applications (SESS'05)*, 2005.
Considering Operational Security Risk During System Development	1/10/07	Carol Woody and Christopher Alberts. *IEEE Security & Privacy*, January/February 2007.
Cybersecurity Strategies: The QuERIES Methodology	8/1/08	Lawrence Carin, George Cybenko, and Jeff Hughes, IEEE *Computer*, August 2008
Enabling Mission Critical Operations Through Mature Implementation	10/11/07	Nadya Bartol, Eric White, Stephanie Shankles, and Michelle Moss. *IAnewsletter*, Vol. 10, No. 2, Summer 2007.
Improving Software Assurance and Top 25 CWE Lists	2/15/10	Bob Ellison and Carol Woody of the Software Engineering Institute discuss software development practices associated with Top 25 Common Weakness Enumeration lists.
Making the Business Case for Software Assurance	4/30/09	Nancy R. Mead, Julia H. Allen, W. Arthur Conklin, Antonio Drommi, John Harrison, Jeff Ingalsbe, James Rainey, and Dan Shoemaker, Software Engineering Institute[1] Special Report CMU/SEI-2009-SR-001, April 2009
Optimizing Investments in Security Countermeasures	9/11/07	Jonathan Caulkins, Eric Hough, Nancy R. Mead, and Hassan Osman. *IEEE Security & Privacy*, September/October 2007.
Process Improvement Should Link to Security: SEPG 2007 Security Track Recap	10/10/07	Security is a very visible issue these days for software. New software products are continuously reported to be vulnerable to attack and compromise; organizations must support an expensive unending update-and-upgrade cycle. Process improvement has been proposed as a mechanism for addressing security challenges, but the Capability Maturity Model Integration (CMMI) approach does not specifically address

		security, so the linkages for the Software Engineering Process Group (SEPG) community are unclear. The security track at the SEPG 2007 conference was developed to provide a forum for identifying the appropriate ties between process improvement and security. This document summarizes the content shared at the conference and identifies several subsequent steps underway toward strengthening those ties.
Risk in the Balance	1/1/05	An effective application-security strategy today must include provision for software vulnerability detection and assessment during the software development process. This practice significantly reduces the risk that vulnerabilities will make it into production – and become corporate liabilities.
Software [In]security: A Software Security Framework: Working Towards a Realistic Maturity Model	10/15/08	Gary McGraw and Brian Chess introduce a software security framework (SSF) to help in planning a software security initiative.
The Protection of Information in Computer Systems	4/17/75	Jerome H. Saltzer, Senior Member, IEEE, and Michael D. Schroeder, Member, IEEE
The Trustworthy Computing Security Development Lifecycle	3/1/05	This paper discusses the Trustworthy Computing Security Development Lifecycle (or SDL), a process that Microsoft has adopted for the development of software that needs to withstand malicious attack. The process encompasses the addition of a series of security-focused activities and deliverables to each of the phases of Microsoft's software development process. These activities and deliverables include the development of threat models during software design, the use of static analysis code-scanning tools during implementation, and the conduct of code reviews and security testing during a focused "security push". Before software subject

		to the SDL can be released, it must undergo a Final Security Review by a team independent from its development group. When compared to software that has not been subject to the SDL, software that has undergone the SDL has experienced a significantly reduced rate of external discovery of security vulnerabilities. This paper describes the SDL and discusses experience with its implementation across Microsoft software. (19 printed pages)
Threat Modeling: Diving into the Deep End	1/3/08	Jeffrey A. Ingalsbe, Louis Kunimatsu, Tim Baeten, and Nancy R. Mead. *IEEE Software*, January/February 2008.
Who Pushed Vendors Toward Better Security?	12/4/08	Mary Ann Davidson, *CIO*, December 4, 2008
Why Application Security Is the New Business Imperative and How to Achieve It	1/1/05	Businesses are being held increasingly accountable for the security of their business applications – by customers, business partners and government. Beyond compliance costs, poor application security can result in heavy downstream remediation and management costs, not to mention productivity problems, hits on revenue and damage to corporate reputations.